Memo of Meeting

Date: February 2, 2000

Representing VeriSign, Inc.
Federal Markets Division
Linthicum MD

Mr. James P. Brandt, Director Federal Markets

Representing FDA

Dr. Steven Solomon, Director, Medical Products Quality Assurance, Office of Enforcement, HFC-240

Tom Chin, Consumer Safety Officer, Division of Compliance Policy, Office of Enforcement, HFC-230

Paul Motise, Consumer Safety Officer, Medical Products Quality Assurance, Office of Enforcement, HFC-240

Jim McCormack, BIMO Program Coordinator, Division of Compliance Policy, Office of Enforcement, HFC-230

Greg Brolund, Associate Director, Office of Information Technology, Center for Drug Evaluation and Research, HFD-70

Liz Chew, Computer Specialist, Office of Information Resource Management, HF-21

The meeting was held at FDA's request, to discuss VeriSign's digital signature and public key infrastructure products and services, in the context of 21 CFR Part 11; Electronic Records; Electronic Signatures. The firm's web site includes VeriSign's document which discusses how the firm's products and services map to specific sections of the rule.

At the start of the meeting we explained that our comments should not be taken as formal FDA assessments of VeriSign's products and services.

During the meeting Mr. Brandt gave a presentation regarding VeriSign's capabilities. This included a overview of the corporation and enterprise PKI

offerings. Mr. Brandt explained that VeriSign is structured to support existing software applications, as opposed to having such applications affect digital signatures and certificates via special "plug-ins." He briefly reviewed the firm's activities in the arena of electronic commerce and applications by federal agencies.

Mr Brandt gave us an overview of VeriSign's public key infrastructure services and how they can be customized so that end user establishments may assume or contract to VeriSign a variety of tasks. With respect to VeriSign's digital certificate authority functions, the firm has 19 processing centers around the world.

Mr. Brandt addressed the firm's certificate practices statement that describes controls the firm uses in the issuance and management of digital certificates.

The VeriSign representative briefly addressed the firm's OnSite architecture, the system of issuing, maintaining and revoking digital certificates using a variety of client configuration options. Mr. Brandt described OnSite as a hybrid of products and services.

During the meeting we also discussed the following particular issues.

Client base. Mr Brandt identified one FDA regulated firm, Johnson and Johnson, among its clients. He commented that the firm purchased a pilot PKI system and expects to launch a major deployment in two years.

Set up time. Mr. Brandt said that typical set up time for a company is about three months -- this was the same for Johnson and Johnson.

Interoperability. Mr. Brandt addressed interoperability in terms of a common point of trust in a PKI system, and in terms of multiple algorithms that VeriSign recognzies. He acknowledged that special customization would have to be done to enable interoperability on a certificate level, for interoperability with competitor certificate authorities. He commented that cross certification is not currently a common method for building digital certificate trust.

Technology maturity. We asked Mr. Brandt to react to industry concerns that PKI technology was not mature enough to confidently adopt. He commented that the technology itself is quite mature, going back to 1984 when PKI systems were first built in military applications. He acknowledged that these systems may be new to some information technology people, and that integration into a user base may be relatively young, but he commented that the technology is, indeed, ready for prime time. He said industry needs to understand PKI better than it currently does.

Legacy systems. Mr. Brandt said VeriSign works with firms that provide software toolkits to enable use of PKIs in legacy systems. He added that his firm would work with clients to help amend legacy applications, in this regard.

Validation audits. Mr. Brandt commented that his firm has been audited with respect to its quality assurance practices and that those reports (subject to non-disclosure agreements) are available to prospective clients. He added that clients such as FDA would be welcome to visit VeriSign's facilities and see the firm's practices and procedures, first hand.

Classes of personal identification (as part of PKI enrollment.) Mr. Brandt explained three different classes. In the first class (retail) the end user owns the verifying information, and uniqueness of name or alias is sufficient to establish individual identification. In the second class aliases are not accepted and a second party provides confirming information (shared liability.) In the third class, the system administrator confirms the individual's identity in person.

Holographic signature. We asked Mr. Brandt whether the term "holographic signature" was widely understood; the term appears in the firm's part 11 paper. He explained that it is not commonly understood, but means an image of a human's scripted name, used in conjunction with cryptographic binding methods.

Intrusion detection. We asked Mr. Brandt about the availability of software and systems to detect attempts at unauthorized access to network computers. We discussed the importance of digital certificate file security and he commented that although his firm does not make such software, intrusion tools and systems are currently available commercially.

Archiving. We discussed the issue of file format changes in migrating from one system to another, and the resulting loss of the ability to verify a digital signature. Mr. Brandt suggested that the file bit string not be altered as part of the migration, but acknowledged the problem.

Corporate affiliation confirmation. We discussed FDA's need, in some circumstances, not only to verify the identity of an individual, but also that individual's affiliation with a corporation. Mr. Brandt briefly explained that such a linkage could be confirmed and made part of the digital certificate.

Mr. Brandt thanked us and the meeting, which lasted about two hours, ended.

P. Motise